Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 04, April 2021: 2150-2156

Research Article

Secure Storage on Cloud using Hybrid Cryptography with Graphical Password Authentication

Dr. P Kavitha[1], Loshıthaa S[2], Monisha M, Ranjana C

[1,2,3,4]Department of Computer science and Engineering, R.M.K Engineering College, Kavaraipettai

Abstract

Authentication service has been advanced by implying advancement in security using cryptography to protect password against data leaking and sniffing. But there is a possibility of shoulder surfing which can lead to data insecurity. Studies shows that graphical or image passwords is more secure because the possibility of guessing is very low. During storage of file, it is encrypted using a single algorithm and there is possibility of data leakage if the encryption algorithm is found. This paper presents a review of a system which aims to provide login security using the graphical password technique and to provide file security using hybrid cryptography, thereby providing the user with highly secured file security system.

Keywords: *Graphical Password, Shoulder-surfing, Hybrid Cryptography, Secure storage*

Introduction

Most of the security system uses text based passwords. For higher security against brute force attack strong password is generated using combination of uppercase and lowercase characters, numerical values and special characters. Strong passwords are randomly generated and does not have specified meaning. Moreover, strong passwords are hard to memorize and recollect. Due to this reason user tried to set easy passwords which is easy to remember. As per the article in computer world, 80% users set such easy password and those can be cracked by hackers within 30 seconds. Based on the Psychological study user is able to remember images with long time span rather than textual words. But most of the image based password security systems are vulnerable to shoulder surfing attack. In shoulder surfing attack, attacker will directly get the information when there is direct contact of the user with the device.

Most of the handheld devices uses pattern based password. This type of authentication system is also vulnerable to shoulder surfing attack. The naked eyes can easily get the credentials or pattern by watching the entered pattern through touch panel or any other technique. Defining easily hackable password or login using password in insecure environment mainly causes loopholes in password security. There is a need of secured password authentication system which overcomes the drawbacks of existing schemes.

Cloud Computing is one of the most liked and diverse topic in today's world. Cloud Storage is available with scalability, cost efficiency, and access of data anytime and anywhere. It is used in various fields like industry, military, college, etc. for various services and also for the storage of large amount of data. It is a combination of number of different technologies. Decrease in cost and load is one of the major advantages of this new technology. There has been an exponential growth in the usage of data, thereby, increased need of data confidentiality which means protecting of data from unauthorized entities. These all factors for different organizations to use this cloud storage and use it as their primary storage service provider. It also restricts the problem of denial of services. But the major drawback in storage of data on the cloud is Security.

This Security concern has to be solved. Encryption is one of the most used methods for the security purpose of data. Different cryptographic algorithms can be used for encryption. But sometimes using single technique or algorithm alone cannot provide high-level security. So we have to introduce a new security mechanism that uses a diferent method.

Literature Survey

The Proposal of new method for storing file with encryption and attributes defined by file owner. The paper proposes the method of storing file along with owner defined attributes and encryption algorithm. The file is decrypted using the attributes defined by owner and key thus ensuring security. The problem in this method is that if a user who knows the attributes can decrypt the file easily.

Mr.H.Gao proposed graphical password scheme using color login. In this color login uses background color which decrease login time. The system developed by Sobrado is improved by combining text with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. The

disadvantage of this system is that it the possibility of accidental login is high and password is too short.

Ms. M Sreelatha proposed Hybrid Textual Authentication Scheme. This scheme uses colors and user has to rate the colors in registration phase. During login phase four pairs of colors and 8*8 matrix will be displayed. As the color rating given by the user, the password will generate. First color shows row number and second shows column number of the grid. The drawback of this system is intersecting element is the first letter of the password. The user has to memorize the rating and order of the colors. So It becomes very hectic to user.

The file transfer between all entities in the network will be end-to-end encrypted, thus ensuring that no entity will get access to sensitive information. In this method only single algorithm is used and only after encryption the file is divided into shards and stored.

System Analysis

2.1 Existing System

File Storage process has many methods for security. The data stored in files is encrypted using a single algorithm and is then stored in cloud. Then the data is decrypted for future use. For login password, mostly text based passwords are used. There are multiple solutions available for the graphical password authentication method. The first solution is to draw the password in the given 2-d grid space. The next technique is to select random images and to arrange it in desired order as password. Some password have direction based graphical authentication. These are the techniques used for password authentication.

Disadvantage: By using this method, security of the data is low. The text based passwords can be easily found by shoulder surfing.

2.2 Proposed System:

Graphical password uses images or colors as a password. Conventional password scheme are sensitive to shoulder surfing, many shoulder resistant graphical password schemes have been proposed. Graphical password is both secure and efficient. Proposed system includes two phases, registration and login & authentication phase.

Registration Phase:

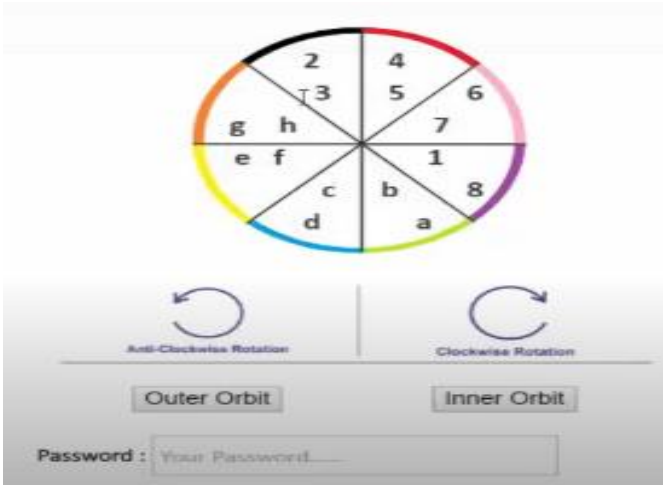
The user has to set his textual password K of length L (4=L=8) characters, and choose one colour as his pass-colour from 8 colours assigned by the system. The remaining 7 colours not chosen by the user are his decoy-colours. And, the user has to register an e-mail address for

re-enabling his disabled account. The registration phase should proceed in an environment free of shoulder surfing. The

system stores the user's textual password in the user's entry in the password table, which should be encrypted by the system.

2.3 Login Phase:

The user requests to login the system, and the system displays a circle composed of 8 equally sized sectors. The colours of the arcs of the 8 sectors are different, and each sector is dentified by the colour of its arc, e.g., the red sector is the sector of red arc. Initially,16 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking the "anti-clockwise" button once.



For secure file storage, we're using hybrid cryptography. Hybrid cryptography uses Advanced Encryption Standard (AES), Blowfish and Twofish.

AES is a symmetric block cipher i.e it uses the same key for both encryption and decryption. AES algorithm uses a substitution-permutation,

or SP network, with multiple rounds to produce ciphertext. AES is a symmetric block cipher i.e it uses the same key for both encryption and decryption.

The main loop of AES performs the following methods:

1. Convert to State Array
2. Transformations
    i. Add Round Key

ii SubBytes

iii Shift keys

iv Mix Columns

3. Key Expansion

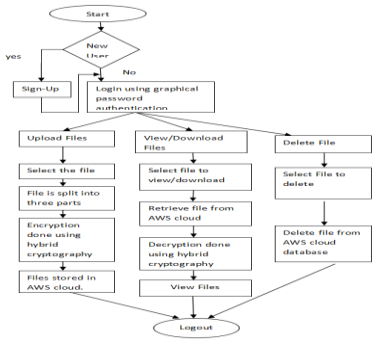
Uses: AES algorithm is used many times and supported on both digital level and physical level.AES is most common security protocol used for various applications.

Blowfish is a symmetric block encryption algorithm designed which is fast, compact, simple and secure. It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte and can run in less than 5K of memory. In key expansion phase, key is converted into several subkeys and in Encryption phase, encryption occurs via 16 round networks. Each round consists of a key dependent permutation and a key & data dependent substitution.

Twofish algorithm is a strong and is one of the algorithm which is recommended as AES.

Design criteria:128-bit symmetric cipher block,having key lengths 128 bit, 192 bit and 256 bit. There is no weak keys,having the efficiency on the software and hardware from different platforms, having a flexible design.

Key schedule: design the key schedule for the ciphers reuse the all same primitives and making it hard to attack both s-boxes and sub key generation process. Two fish is fast and can perform 17.8 clock cycles per byte. It has minimal table requirements and make it efficient on 8 bit CPU's suitable for hardware trade offs and smart cards.



System Architecture:

Modules:

User Side:

Registeration Scenario:

Firstly the user enters the website. If the user does not have a account the he/she creates a new account else the user logins using the credentials.

Then user logs in to the website in a safe environment. The user can then upload the files that has to be stored securely.

Upload Scenario:

When user uploads a file the file is divided into three equal parts and each part is encrypted using different algorithms and is then stored in AWS.

Then user can view the uploaded files and download the files whenever required. While downloading or viewing , the file is retrieved from AWS and is then decrypted before displaying it to the user.

Admin Side:

The admin has created a database to store the user details for login purpose. Then database has been created to store the files which is to be stored securely.The file which is to be stored is first encrypted before storing in the database and then stored for future purpose.We can upload, view, download or we can view the data which is in the database.The data will be decrypted for the user's need.

Result

By using Graphical password technique, password involves characters along with the colours which has lead to Secure login and shoulder surfing attack has been prevented. The file storage process uses the hybrid cryptography method which is combination of three algorithm is used for single file provides high security. Thus graphical password authentication and hybrid cryptography method has created a highly secure file storage method.

Conclusion

Graphical Password Authentication has been proven to be shoulder-surfing-proof authentication system because users will use text along with colours as their password. Cryptographic algorithms play a very important role in Network security. The hybrid cryptography method provides high data security. In this process, we have used three encryption algorithms: AES, Blowfish and Two fish. These algorithms are comparitively faster than other algorithms. In future, some more algorithms can be used for the security purpose.

References

[1] Madigan, S. “Picture Memory”, In J. C. Yuille, Imagery, Memory and Cognition (PLE: Memory): Essays in Honor of Allan Paivio, Psychology Press, 2014, pp. 65-66.

[2] Wu, T. S., Lee, M. L., Lin, H. Y., & Wang, C. Y. “Shoulder-surfing-proof graphical password authentication scheme”, International Journal of Information Security, 13(3), 2014, pp.245–254.

[3] H. Xiong and J. Sun, ‘‘Comments on verifiable and exculpable outsourced attribute–based encryption for access control in cloud computing,’’ IEEE Trans. Depend. Sec. Comput., vol. 14, no. 4, pp. 461–462, Jul. 2017.

[4] Sarohi, H. K., & Khan, F. U. “Graphical Password Authentication Schemes: Current Status and Key Issues”, IJCSI International Journal of Computer Science Issues ,2013, pp 427-443.

[5] Haichang, G., Zhongjie, R., Xiuling, C., Xiyang, L., & Aickelin, U. “A New Graphical Password Scheme resistant to shoulder surfing”, International Conference on CyberWorlds. University of Nottingham, 20-22 October 2010.

[6] S. Farmand and O. B. Zakaria, "Improving graphical password resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4)," 2010 2nd IEEE International Conference on Information Management and Engineering, Chengdu, 2010, pp. 644- 650.

[7] J.-S. Su, D. Cao, X.-F. Wang, Y.-P. Sun, and Q.-L. Hu, ‘‘Attribute–based encryption schemes,’’ J. Softw., vol. 22, no. 6, pp. 1299–1315, Jun. 2011.

[8] J. Liu, X. Huang, and J. K. Liu, ‘‘Secure sharing of personal health records in cloud computing: Ciphertext–policy attribute–based signcryption,’’ Future Gener. Comput. Syst., vol. 52, pp. 67–76, Nov. 2015.

[9] L. Wu, Y. Zhang, K.-K.-R. Choo, and D. He, ‘‘Efficient and secure identitybased encryption scheme with equality test in cloud computing,’’ Future Gener. Comput. Syst., vol. 73, pp. 22–31, Aug. 2017.

[10] Q. Xu, C. Tan, Z. Fan, W. Zhu, Y. Xiao, and F. Cheng, ‘‘Secure multi– authority data access control scheme in cloud storage system based on attribute–based signcryption,’’ IEEE Access, vol. 6, pp. 34051–34074, 2018.

[11] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. L. Wei, and P. Hong, ‘‘RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage,’’ IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 953–967, Apr. 2017